September 16, 2016

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Ex Parte Presentation, *Protecting the Privacy of Customer Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

Dear Ms. Dortch,

CTIA[1] submits this letter in further response to the Notice of Proposed Rulemaking ("NPRM")[2] in the above-mentioned proceeding. CTIA appreciates the Commission's goal of protecting the privacy and data security of broadband consumers, but continues to have concerns that the Commission's Proposed Rules suffer from serious infirmities.

In recent submissions, Paul Ohm, Public Knowledge, New America's OTI ("OTI"), and others (collectively, "Pro-NPRM Commenters") have raised several new arguments to counter CTIA's and others' objections to the Proposed Rules. Their arguments, however, fail to resolve gating questions that have plagued this proceeding from the beginning—most notably, (1) why the Commission has proposed departing from the Federal Trade Commission's ("FTC's") effective, technology-neutral, sensitivity-based

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America's competitive and world-leading mobile ecosystem. The association also coordinates the industry's voluntary best practices and initiatives and convenes the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) ("NPRM").

approach to data protection; (2) whether, in the alternative, the Proposed Rules can be analogized to other "sectoral" privacy regimes; (3) whether the Commission has statutory authority to regulate information other than "individually identifiable customer proprietary network information"; (4) whether the Proposed Rules materially advance a cognizable and record-based privacy interest; and (5) whether the Commission has given adequate consideration to the uncontested positive, pro-consumer, pro-competitive effects of information processing by Internet Service Providers ("ISPs") like CTIA's members.[3]

Below, CTIA addresses some of the new arguments from the Pro-NPRM Commenters on these questions. The Commission should not accept the Pro-NPRM Commenters' invitation to ignore clear gaps in the record or to exceed statutory and constitutional limits on the Commission's authority. CTIA also reiterates that if the Commission is committed to pressing forward, it should at the very least follow a more prudent, cautious approach, which is described at greater length below.

The Commission Should Adopt a Sensitivity-Based Approach.

As many commenters including CTIA and even the FTC Staff have proposed, any final rules the Commission adopts should provide differing levels of protection based on the sensitivity of the underlying information that is being used or disclosed, with heightened protection (*i.e.*, opt-in consent) reserved for only intentional uses and disclosures of sensitive information.[4] Such an approach would ensure that the FCC's privacy regime has some nexus to privacy concerns and is consistent with other effective, technology-neutral privacy regimes—including the FTC's and those established by and under various other federal laws. There are numerous benefits to such an approach, as CTIA and others have explained in prior submissions.[5] Ohm departs from this consensus approach by recommending that the Commission require

[3] CTIA does not intend via this submission to withdraw or waive any of the other arguments raised in its Opening or Reply Comments in this proceeding.

[4] *See, e.g.*, CTIA Reply Comments at 8-9; FTC Comments at 8, 22-23. *See also* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* 47(Mar. 2012) ("*FTC Report*") at 47-48 (explaining that opt-in consent for first-party marketing using sensitive data should be limited to when "a company's business model is *designed to target* consumers based on sensitive data") (emphasis in original).

[5] *See* CTIA Reply Comments at 8-9; CTIA Opening Comments at 94-98.

opt-in consent for the use and disclosure of virtually all information by ISPs for virtually all purposes.[6] He fails, however, to offer a reasonable justification, either statutory- or policy-based, for doing so.

Ohm's primary argument in favor of the Commission's approach is based on a syllogistic fallacy: because all data covered by sectoral laws are intrinsically sensitive (the "big" proposition), and because Section 222 is a standard privacy law for the telecommunications sector (the "small" proposition), the Commission has authority under Section 222 to treat all data in the sector as sensitive.[7] CTIA debunks the purported similarity between the Proposed Rules and other sectoral privacy regimes at greater length below. But even if the "big" proposition were generally correct, the "small" proposition fails as a simple statutory matter: Section 222 does not restrict the use and disclosure of all customer information obtained by providers in the telecommunications sector. Instead, Congress drafted Section 222(c) to restrict the use and disclosure of a *specific category* of customer information that Congress deemed uniquely sensitive because of a provider's provision of telecommunications service (*i.e.*, individually identifiable customer proprietary network information ("CPNI")), which Congress enumerated and defined in Section 222(h).

To justify the Commission's attempts through this proceeding to expand the scope of customer data covered by Section 222, Ohm engages in a sleight of hand. He conveniently and entirely ignores the distinction that Congress made when it intentionally omitted during conference committee negotiations an earlier catch-all provision that would have allowed the Commission to expand the scope of customer information covered. Moreover, Ohm's approach would lead to absurd results. Under Ohm's interpretation, the Proposed Rules would define CPNI to include data that are obviously not sensitive or uniquely collected by ISPs—for example, a customer's IP address.[8] Indeed, the Commission's Proposed Rules expressly extend far beyond the statutory definition of CPNI to include the broader category of "customer proprietary information" which the Commission defined itself.

---

[6] Ohm Ex Parte at 4 (July 28, 2016).

[7] *Id.*

[8] *NPRM* ¶ 41.

Ohm also ignores Congress's decision to require opt-in consent in only two very specific cases: in connection with (1) the use or disclosure of call location information concerning the user of a CMRS device or IP-enabled voice service for non-specified purposes, and (2) the use of automatic crash notification data for purposes other than such notification. The plain language of the statute makes clear that Congress did not intend to require providers to obtain opt-in consent for the use and disclosure of CPNI in other instances.[9]

Ohm also argues that distinguishing between sensitive and non-sensitive information is too difficult, and therefore all information should be treated as sensitive.[10] But in this respect too, he diverges from the FTC, which, after a lengthy and comprehensive process, identified certain specific information as sensitive (*i.e.*, Social Security numbers, children's information, health information, financial information, and precise geolocation information), and recommended heightened protection (*i.e.*, opt-in consent) for uses and disclosures of such information in many, but not all, instances. The FTC's approach would not be difficult for ISPs to implement.[11] First, the FTC has established guidelines that companies may follow in drawing lines to determine when opt-in consent is required.[12] Second, prior to the reclassification of broadband, many ISPs operated under the FTC's technology-neutral, sensitivity-based regime, and many entities with access to the same data continue to operate under this regime today. Third, despite claims to the contrary, sensitivity-based rules would not require ISPs to examine data traveling over their networks to determine which data were sensitive.[13]

---

[9] CTIA Opening Comments at 28-29 (discussing how legislative history of Section 222 shows Congress intended to limit the scope of customer information covered by Section 222 to specifically enumerated categories of information).

[10] Ohm Ex Parte at 4.

[11] Moreover, contrary to consumer groups' recent assertion in their ex parte dated September 7, 2016, compliance with sensitivity-based rules modeled on the FTC's approach would not be difficult for the Commission to oversee, as such rules would apply only when an ISP *used* sensitive data to target consumers based on inferences drawn from the sensitive nature of the data. Consumer Groups' Ex Parte at 3 (Sept. 7, 2016).

[12] *FTC Report* at 47-48.

[13] The proposed definition of "customer proprietary information" appears to capture categories of information that ISPs could collect from subscribers through traditional, offline non-network channels (*i.e.*, through traditional mail-based marketing campaigns). The use of such information was neither opposed nor even raised by commenters in this proceeding. Clarifying

That is so because such rules requiring opt-in consent would be triggered only if an ISP were to launch a marketing campaign to target customers based, in part, on inferences drawn from sensitive personal information, and not simply by virtue of providing the underlying broadband service.

Ohm also discourages the use of a multistakeholder process to define what data are sensitive.[14] His objections, however, center around a general distrust and dislike of multistakeholder processes, and he does not offer any reason why the issue of data sensitivity would be less suited to this process than other issues, such as drones or mobile app transparency.[15] Moreover, the Administration has repeatedly advocated the use of multistakeholder processes to build consensus around flexible best practices and guidelines, which are preferable to regulations and legislation for the fast-paced and ever-evolving digital ecosystem in which both consumers and companies operate. CTIA notes, however, that an alternative approach—although by no means necessary—would be for the Commission to follow its past practice when confronting similarly complex issues. Specifically, based on the extent of this record and the clear impossibility of reaching consensus *now*, it makes eminent sense to phrase final rules broadly (*i.e.*, using "sensitive" in the text of the rules without defining the concept further). Doing so would preserve flexibility for the Commission to flesh out its rules in further proceedings, even based on an FNPRM.

The Proposed Rules Cannot Be Justified by Analogy to "Sectoral" Privacy Regimes.

As noted, Ohm repeatedly analogizes both Section 222 itself and the Proposed Rules to privacy regimes in other sectors to defend against attacks that asymmetric

---

language regarding such information collection and use would be helpful. This distinction also highlights the need to distinguish between uses and disclosures of sensitive and non-sensitive information to avoid amplifying the asymmetric, anti-competitive nature of the proposed rules with respect to such information collection.

[14] Ohm Ex Parte at 5.

[15] Indeed, Ohm's objection is curious, given how similar multistakeholder processes are to the FTC's approach in developing the *FTC Report*, which involved multiple workshops and meetings with—and comments from—a wide variety of stakeholders. *FTC Report* at i-iv (describing how the FTC drafted the report after holding multiple workshops, consulting with other federal agencies, and considering comments from over 450 stakeholders, including privacy advocates, technologists, consumers, and businesses).

regulation of ISPs is unconstitutional or arbitrary and capricious.[16] But even leaving aside the statutory argument, set forth above, that Section 222 cannot support restrictions on the uses and disclosures of all information collected by telecommunications providers, Ohm's analogy is even more flawed when the relevant "sector" is translated from the voice ecosystem to the online ecosystem. Specifically, in the 1990s, when the statute was enacted, the market for voice service featured characteristics (most notably, the closed nature of the market and the exclusive access of voice providers to certain data about their customers, *i.e.*, CPNI) that made it susceptible to sector-wide regulation (which, to reiterate, Section 222 nonetheless did not impose). In contrast, the broadband market has characteristics, discussed below, that make it uniquely *unsuitable* for sectoral regulation. In light of those characteristics, the Proposed Rules bear no resemblance to traditional sectoral privacy regimes, and they therefore would not survive judicial review.

Ohm offers several examples of "class[es] of information" that have "justif[ied]" sectoral privacy regulation in the past—including health information, student records, and credit reports.[17] But as Ohm has recognized in his scholarship, these categories of information share several critical similarities, two of which are quite obviously lacking here.

First, these categories of information generally involve unique risk of harm to subjects.[18] Second, for each category of information that merits sectoral regulation, there should be identifiable and limited points of entry into the stream of commerce.[19] Neither of these conditions—unique risk of harm or amenability to control—is present here. With respect to the first condition, the Proposed Rules are aggressively over-inclusive, encompassing not just sensitive information (or even just arguably sensitive

---

[16] Ohm Ex Parte at 4; Ohm Testimony at 6 (June 10, 2016).

[17] Ohm Testimony at 5.

[18] *See* Paul Ohm, *Sensitive Information*, 88 S. Cal. L. Rev. 1125, 1161 (2015) ("The first, and perhaps only necessary, factor [for determining sensitive information] is connection between the category of information and harm. Information is . . . sensitive if adversaries . . . can use it to cause harm to data subjects or related people."); *see also FTC Report* at 47.

[19] *See* Ohm, *Sensitive Information*, 88 S. Cal. L. Rev., at 1168 (describing that sectoral privacy laws protect information shared between individuals and "particular parties" that "owe a duty of confidentiality to [the] data subjects due to special relationships").

information) but also vast swaths of non-proprietary, non-sensitive information (*e.g.*, IP address, as well as customer name and address). And with respect to the second condition, the rules encompass only ISPs, leaving edge providers, data brokers, and appenders—who have access to the same, if not more, information—subject to a different standard under the FTC's privacy regime. As CTIA has explained, these carve outs are fatal from a constitutional and regulatory perspective. Indeed, in *Sorrell v. IMS Health, Inc.*,[20] the Supreme Court emphasized the distinction between the HIPAA Privacy Rule, on the one hand, which "advanced . . . asserted privacy interests by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances," and the challenged Vermont law, which "made prescriber-identifying information available to an almost limitless audience" with the exception of "a narrow class of disfavored [commercial] speakers" in holding that the latter was unconstitutional.[21] So too here, the fact that so many elements of "customer proprietary information" will be available to an almost limitless audience of providers in the same ecosystem shows that the Proposed Rules do not create a coherent sectoral privacy regime that justifies their restriction on speech.

Even Public Knowledge appears to have recognized that drawing distinctions between providers within the online ecosystem is "arbitrary," will generate "customer confusion," and otherwise is not the "best policy" outcome.[22] But Public Knowledge bizarrely claims that the problematic distinction is Congress's statutory delineation between ISPs that utilize cable systems and ISPs that do not—rather than the Commission's asymmetric regulation of ISPs vis-à-vis edge providers. Public Knowledge cannot have it both ways; if harmonization across ISPs is desirable to avoid customer confusion, then harmonization throughout the ecosystem is desirable for the same reason.

Moreover, Public Knowledge also fails to grapple with the characteristics of the relevant service markets that undermine the rationale for discriminatory restrictions on ISPs. As just one example, despite multiple submissions, Public Knowledge has never addressed mobile providers' deliberate campaigns to drive down switching costs. Nor

---

[20] 564 U.S. § 552 (2011).

[21] *Id.* at 573.

[22] Public Knowledge Ex Parte at 3-4 (unpaginated) (July 26, 2016).

has Public Knowledge addressed the economic and behavioral realities that make switching costs considerably higher in the markets for e-mail and social networks than in the market for mobile broadband Internet access service.[23]

The Proposed Rules Unambiguously Exceed Limits Regarding the Scope of Data Under Section 222.

CTIA and others consistently have argued that the Commission lacks statutory authority under Section 222, among other things, to regulate the use or disclosure of, or access to, information other than individually identifiable CPNI. Any other reading is inconsistent with the text of individual subsections of Section 222 and would render the statute structurally and holistically incoherent. In reply comments and ex partes, the Pro-NPRM Commenters finally attempt to use traditional tools of statutory interpretation to argue that Section 222 can encompass customer information beyond individually identifiable CPNI—including both "customer proprietary information" and de-identified CPNI—but their efforts fall short.

First, as CTIA has demonstrated, Section 222(a) unambiguously cannot be interpreted to vest the Commission with authority to protect information beyond CPNI. That is so because to interpret Section 222(a) otherwise would be inconsistent with the legislative history, effectively would render Sections 222(e) and 222(g) null, would cause absurd results related to disclosures under Section 222(d), and would be tantamount to a novel discovery of expansive power within a previously dormant statutory provision.[24] Rather than address these difficulties, OTI and others erroneously suggest that interpreting Section 222(a) to state policy rather than confer authority is impermissible under the canon against surplussage.[25] But this argument ignores the fact that context matters, as *Verizon v. FCC* makes clear.[26] Whatever the merits of *Verizon*'s *holding*, the court's *reasoning* confirms that provisions of the Telecommunications Act certainly can be interpreted as general statements of policy, rather than as grants of additional authority. Specifically, in *Verizon*, the D.C. Circuit found that Section 706(a) of the Act is

[23] CTIA Reply Comments at 54-56; CTIA Opening Comments at 113-16.

[24] CTIA Reply Comments at 17-19; CTIA Opening Comments at 25-35.

[25] *See, e.g.*, Reply Comments of OTI at 7-8.

[26] 740 F.3d 623 (D.C. Cir. 2014).

ambiguous as to whether it functions as a conferral of substantive authority or as a pure statement of policy.[27] The court resolved the ambiguity by reference to the inclusion of Section 706(a) of words suggesting a regulatory intent, such as "price cap regulation," "forbearance" and other "regulating methods."[28] While Section 222(a) is likewise ambiguous, it lacks the regulatory terminology present in Section 706(a). Given this distinction, and in light of the intractable problems of statutory interpretation identified above, Section 222(a) cannot reasonably be deemed as anything other than a policy statement.

Second, despite the Pro-NPRM Commenters' arguments to the contrary, Section 222(c) cannot be interpreted to permit restrictions on the use and disclosure of de-identified CPNI. Public Knowledge's argument—that allowing ISPs to use de-identified information somehow deprives customers of the control that Congress meant to give them over their personal information—makes no sense. De-identified data, by definition, comprise information that does not identify customers. Therefore, it is no longer "customer" information. Moreover, contrary to Public Knowledge's assertion, the use of de-identified information will not create a "windfall" for ISPs; it will lead to customer benefits. The Telecommunications Act was designed to make broadband Internet access services more available and affordable. If ISPs are able to innovate and offer or deliver new products and services, such as advertising, they will generate new revenue streams to fund their deployment of broadband infrastructure. These are significant costs that consumers, other carriers, or the Universal Service Fund otherwise would bear. Allowing ISPs to use de-identified data to provide new products and services is therefore precisely the kind of innovation that the Act was meant to encourage.

Even if the Commission agrees with Public Knowledge's argument as a matter of policy (which it cannot adopt for procedural reasons), restrictions on the use of non–individually identifiable CPNI are foreclosed by the statute in any event. Ohm misinterprets Section 222(c), suggesting that the perceived structural similarity between Section 222(c)(1) and (c)(3) means that Congress contemplated only two categories of customer information: "individually identifiable CPNI" and "aggregate customer

[27] *Id.* at 635, 637-38.

[28] *Id.* at 637-38.

information."[29] Ohm's argument fails as a matter of statutory interpretation, however. Ohm ignores the fact that Section 222(c)(1) refers to the collection or receipt of CPNI generally and then imposes restrictions only with respect to "individually identifiable" CPNI, a subset of CPNI.[30] Thus, the statute on its face makes clear that Congress did not create a binary distinction between "CPNI," on the one hand, and "aggregate customer information," on the other. Indeed, a proper reading of the statute shows that Congress intended to impose restrictions not on the use and disclosure of CPNI generally, but on only a subset of CPNI that was sensitive because it could reveal certain information about the customer—namely, "individually identifiable" CPNI.[31]

---

[29] Ohm Ex Parte at 2; *see also* Reply Comments of OTI at 9-13.

[30] *See* 47 U.S.C. § 222 (c)(1). Likewise, Section 222(e) creates yet another category of information, subscriber list information, and Section 222(h)(1) defines CPNI without regard to whether the information does or does not identify an individual, further suggesting that "individually identifiable" must be interpreted as a limiting compound modifier in Section 222(c)(1).

[31] Ohm appears to be completely unaware of the historical context in which Congress drafted Section 222 and that is critical to understanding the statute. Congress drafted Section 222, in large part, to foster competition in the voice services market in the wake of the Bell divestiture. Section 222(c) refers to CPNI and aggregate customer information because the Bell operating companies' (BOCs') obligations with respect to these two types of data differed: BOCs did not need to share CPNI with competing providers, except at customer request, but—in order to facilitate new carriers' entry into the market—BOCs *did* need to share aggregated CPNI with competing providers at the same price and under the same conditions as BOCs did with their own enhanced services. Section 222(c)(3) was designed to codify that arrangement. *See In re Implementation of the Telecommunications Act of 1996*, Second Report and Order and Further *NPRM*, 13 FCC Rcd 8061, ¶147 (1998) ("*CPNI Second Report and Order*") ("As part of the *Computer III* rules established prior to the 1996 Act, the Commission requires the BOCs and GTE to provide aggregate customer information to enhanced service providers when they share such information with their enhanced service affiliates. The Commission also requires the BOCs to provide aggregate customer information to CPE suppliers when they share such information with their CPE affiliates."); *see also CPNI Second Report and Order* ¶152 ("Section 222 requires only that when LECs seek to target customers based on aggregate customer information which create generalized 'profiles' of groups of customers likely to respond favorably to service offerings outside their existing service, they must also make these group profiles available to their competitors. In this way, Congress sought to rectify the LECs' advantage in scope and wealth of CPNI, while at the same time not compromising customers' privacy interests."). Thus, the structure of Section 222(c) was driven by efforts to create the appropriate competitive framework for BOCs post-divestiture and not to create a "binary dichotomy" between two types of data for purposes of privacy protection.

Moreover, Ohm's interpretation of the phrase "individually identifiable" would yield absurd results. For instance, a customer record devoid of *any* identifying information (*e.g.*, zip code and type of service) is not "individually identifiable" CPNI. But this record standing on its own also does not constitute "aggregate customer information," because Congress defined "aggregate customer information" as "collective data that relates to a group or category of services or customers from which individual identities and characteristics have been removed." In addition, Ohm states that, "Subsection 222(c)(1) refers to 'individually identifiable' CPNI—not '*reasonably* individually identifiable' CPNI," and he asserts that, "[t]he unadorned phrase 'individually identifiable' means, quite literally, information that can possibly be identified with an individual."[32] He concludes that this means Subsection 222(c) captures "any information that could be reidentified as an absolute, technical matter, regardless of business process protections that might reduce the risk of reidentification."[33] Yet this would preclude any number of legitimate and essential business operations using de-identified CPNI that ISPs have ensured, through enforced administrative controls, will not be re-identified. And if administrative controls were inadequate to de-identify CPNI, then *any* CPNI that theoretically could be re-identified through herculean technical efforts—no matter how unlikely or impractical—would be CPNI. This interpretation would render the phrase "individually identifiable CPNI" virtually meaningless.[34] In any event, as CTIA explained in its Reply Comments, "research reflects that de-identification is highly effective when executed correctly and that re-identification is a complex process requiring both an alternative data source and a highly skilled expert to have any chance of success."[35]

---

[32] Ohm Ex Parte at 3.

[33] *Id.*

[34] The FTC has noted this risk that the Commission's proposed definition of "personally identifiable information" posed, and it recommended that "[w]hile almost any piece of data could be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology." FTC Comments at 9. As explained below, this is precisely the approach to de-identification that the FTC has taken, focusing on whether re-identification is "reasonable" under the circumstances.

[35] CTIA Reply Comments at 22. Consumer groups asserted that "researchers have been able to re-identify individuals" using de-identified data. Consumer Groups' Ex Parte at 2. The examples they cite, however, involved technical experts who used sophisticated technological tools and had access to supplemental datasets. *Id.* The FTC's three-part test, described above, requires

In addition to his statutory argument that Section 222(c) limits the use and disclosure of *any* CPNI that possibly could be re-identified, Ohm also argues that this strained interpretation comports with the FTC's approach. Specifically, Ohm argues that the *FTC Report* "speaks only of technical rather than process protections," and he cites a sentence from the report that states, "[d]epending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields," and so forth.[36]

Ohm is incorrect. The *FTC Report* establishes the following three-part test to use in determining whether data would not be *reasonably* linkable to a particular consumer (*i.e.*, whether the FTC privacy framework will apply): (1) the company must take *reasonable* measures to ensure that the data are de-identified; (2) the company must publicly commit to maintain and use the data in a de-identified fashion, and not attempt to re-identify the data; and (3) if a company makes such de-identified data available to other companies, it should contractually prohibit those companies from attempting to re-identify the data.[37] Ohm actually misstates the first part of this test—taking "reasonable measures to ensure that data is de-identified"—and instead cites one of the possible types of "reasonable measures"—technical protections—that companies could use to meet this prong. Specifically, the FTC states that one "reasonable measure" to use "may be" one of "a variety of technical approaches."[38] The *FTC Report* does not say that this is the only "reasonable measure" that a company may take, however. Indeed, the FTC states that the test is whether the "*reasonable* measures" the company takes give the company "a *reasonable* level of justified confidence that the data cannot *reasonably* be used to infer information about, or otherwise be linked to" an individual.[39] Thus, the touchstone of the FTC's test is "reasonableness"—not, as Ohm argues, absolute technical certainty. Moreover, in arguing that the *FTC Report* speaks only to technical, and not administrative, processes to de-identify data, Ohm incorrectly cites only the first prong of the test, ignoring the

---

both technical *and* administrative controls to sufficiently de-identify data and therefore precludes the kind of activity that these technical experts engaged in to re-identify data.

[36] Ohm Ex Parte at 3 n.7 (citing *FTC Report* at 21).

[37] *FTC Report* at 21.

[38] *Id.*

[39] *Id*. (emphasis added).

administrative controls in prongs two and three. Yet the FTC included administrative controls precisely because it was *not* requiring companies to take measures that ensure to an absolute technical certainty that data cannot be re-identified. It recognized that "reasonable measures" may not be foolproof and that therefore administrative controls are also important.

The Commission Should Rely on Only Cognizable Privacy Interests Supported by the Record.

Under both the APA and the First Amendment, the Commission must identify the privacy interests that the final rules are intended to advance—and in the case of the latter, the Commission will be held to a particularity requirement and strict means-ends testing.[40] Ohm's and OTI's recent submissions rely on both abstract concepts of privacy and purely theoretical threats to support the Commission's interest in adopting the Proposed Rules. Ohm, for his part, invokes seemingly weighty notions of privacy in letters, documents, and reading lists, but these privacy interests are a red herring here.[41] And OTI goes to great lengths to cite academic literature to suggest that the Commission has an interest in regulating collection, processing, use, and disclosure of information, to prevent all possible subjective and objective privacy harms.[42] But to justify the rules, the Commission must identify a *legally cognizable* privacy interest that inheres to the statute, and must propose rules that substantially advance that interest. OTI's asserted interests fail in each respect.

To be clear: CTIA has never claimed that there are not significant privacy concerns in the online ecosystem. Indeed, CTIA's members are committed to protecting the online privacy and data security of their customers, and have taken robust, meaningful steps to provide such protections; doing so is simply good business practice. Nor has CTIA ever claimed that the protection of privacy cannot be a legitimate state interest. Instead, CTIA has emphasized that, as a matter of settled doctrine, the state's interest in protecting privacy must be specifically and narrowly defined, because the protection of privacy imposes economic and other costs by

---

[40] *E.g.*, *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234-35 (10th Cir. 1999).

[41] *See* Ohm Testimony at 4-5.

[42] *See* Reply Comments of OTI at 27-32.

inhibiting the free flow of information. For this reason, courts generally have been hesitant to expand the state's interest in protecting privacy beyond certain specific interests: (1) protection against disclosure to unknown third parties; (2) protection in the home; and (3) protection from uniquely vexatious or harassing communications.[43] The FTC and various legislatures also have propounded an additional interest in the protection of uniquely sensitive information. Each of these interests has valid legal pedigree.

In contrast, OTI and Ohm are through the looking glass, claiming that the Commission can rely on various strands of academic privacy literature to combat hypothetical practices that, they speculate, after a chain of unlikely events, could result in a dystopic scenario of surveillance and self-censorship. The Commission should not follow them down the rabbit hole. Any purported privacy interest that the Commission asserts in this proceeding will be rigorously tested on review, because the regulations impose speaker-based and content-based burdens on speech, and the more expansive the purported privacy interest, the more speech will be swept in, and the greater the First Amendment harm.

In his testimony regarding the Proposed Rules, Ohm describes the stakes of this proceeding in stark terms, claiming that "almost nothing receives the heightened protection for privacy given to the content of our conversations" and that "[n]o power in the technological history of our nation has been able until now to watch us read individual articles, calculate how long we linger on a given page, and reconstruct the entire intellectual history of what we read and watch on a minute-by-minute, individual-by-individual basis."[44]

The Commission should look past these rhetorical flourishes. First, these concerns lack any nexus to Section 222, which reflects Congress's concern about a particular category of information that derives from the provider-customer relationship. Second, Ohm ignores the practical reality that it would be cost prohibitive for ISPs to engage in constant deep packet inspection ("DPI") or other forms of collection that animate his

[43] *See* CTIA Opening Comments at 84-85 and accompanying footnotes.

[44] Ohm Testimony at 5.

advocacy—and indeed ISPs have strong incentives not to do so.[45] Third, the invocation of these interests leads to absurd mismatches of ends and means in the online ecosystem. For example, it makes little sense to rely on the privacy of reading lists to subject ISPs to asymmetric regulation, when the raison d'être for the most popular social networks is to encourage the sharing of such information—not to mention that the business model of such social networks is to monetize that information and that social plug-ins have amplified social networks' already vast information collection and processing capabilities.

OTI similarly strays far afield by relying on privacy interests that include not just control of information and prevention of actual and likely harm, but also protection against theoretical and hypothetical threats to autonomy, dignity, and expression. CTIA does not contest that these are valuable interests, or that they can be advanced through the protection of privacy. But they are inadequate to support the Proposed Rules for several reasons.

First, the Commission lacks any record that ISPs' practices are creating a threat to broadband customers' autonomy or dignity—in contrast to the record developed in the *Pretexting Order*, where there was record evidence of emerging specific practices that were exposing consumers to substantial risk of physical harm or harassment, and where the Commission was regulating the unique locus of harm (sharing with independent contractors and joint venturers). Nor is there any record evidence that ISPs' practices are encouraging self-censorship; to the contrary, Internet usage continues to increase, including in the form of online activities that directly involve sensitive information, notwithstanding any concerns they may have about online privacy.[46]

Second, insofar as OTI is motivated by concerns with information *collection*, it misses the statutory mark. Section 222 imposes no limitations on collection whatsoever; it restricts only use and disclosure/access. Moreover, as discussed above, there is no

---

[45] *See* CTIA Reply Comments at 29-30; Feamster Comments at 6 (explaining that focus on DPI is a "red herring" because it is not widely deployed and prohibitive costs make extensive retention and analysis practically infeasible).

[46] *See* CTIA Reply Comments at 32-33; CTIA Opening Comments at 67-71.

evidence that ISPs are—or ever will—engage in rampant information collection, or that ISPs have unique data collection capabilities vis-à-vis other edge providers.

Third, OTI's discussion of the privacy threats that result from data *processing* are no more availing. OTI's emphasis on the emerging practice of aggregating "disparate datasets that have information about the same individual" is misplaced,[47] both because Section 222 does not restrict the use or disclosure/access of aggregate information, and because Section 222 restricts the use or disclosure/access of only individually identifiable information that an ISP obtains by virtue of providing service. Accordingly, the Proposed Rules will have no effect on the rich secondary market for data brokers and appenders, and, indeed, may very well strengthen the position of those entities vis-à-vis ISPs. Separately, OTI's assertion that "[s]econdary uses [of information] are another practice that causes harm"[48] is inconsistent with emerging legal and business norms—not only in the United States, but also in the European Union—that first-party internal processing is generally considered contextually permissible without opt-in consent.[49]

Finally, CTIA acknowledges that information *dissemination* can create privacy concerns. But even that uncontroversial proposition notwithstanding, OTI's statement that "this type of harm needs little explanation"[50] ignores the procedural requirements that govern rule-making proceeding under the APA. Specifically, agencies are required to provide fulsome explanations to justify their rules to ensure that they have engaged in reasoned decision-making. And here, the Proposed Rules regarding disclosure and access are clearly wanting, because the Commission has failed to explain its uniform treatment (*i.e.*, opt-in consent requirement) for both disclosures and access, on the one hand, and for virtually all recipients (*e.g.*, agents, vendors, independent contractors), on the other.

---

[47] Reply Comments of OTI at 28.

[48] *Id.* at 29.

[49] *See FTC Report* at 40; EU GDPR, Art. 21, ¶¶ 47-50.

[50] Reply Comments of OTI at 30.

The Commission Cannot Ignore the Costs of the Proposed Rules, Including Higher Retail Prices, Less Innovation, and Reduced Competition.

Even if they were correct about the privacy benefits that could accrue from the Proposed Rules (which they are not), the Pro-NPRM Commenters still fail to address the other side of the ledger (*i.e.*, the countervailing interests to the protection of privacy). As CTIA and others have explained, the Proposed Rules would have a variety of harmful effects on multiple service markets and, ultimately, consumers—including the majority of consumers who are privacy neutral, and therefore will experience no benefit from the Proposed Rules at all.[51] These harms include both compliance costs, which are likely to be particularly pronounced on small providers, and indirect costs and lost revenue. A full recapping of these harms is unnecessary here, but the Commission must at minimum account for the following likely effects as it formulates final rules.[52]

The Proposed Rules will prevent ISPs from being able to offer increasingly customer-friendly products, services, and bundles entirely within the provider-customer first-party relationship. Specifically, ISPs previously have used customer information to market new offerings, ranging from device cases and screens to new services or joint promotions, to customers.[53] By engaging in further internal data processing, ISPs will be able to tailor and refine such offerings to better match customer preferences. Their doing so also will enhance competition, as providers seek to lure away customers by offering more innovative packages and bundles. Under both the FTC's and EU's respective privacy regimes, such processing and marketing would be considered contextually permissible with implied consent; under the Proposed Rules, providers would be required to obtain opt-in approval—which many customers might not provide simply due to inertia and other transaction costs.

---

[51] *See* Wright Comments at 16-20.

[52] *See, e.g.*, *Motor Vehicle Mfrs Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (describing that agencies must rely on factors intended by Congress, consider important aspects of problem to be addressed, and provide cogent explanations for decision making); *Int'l Union, United Mine Workers of Am. v. MSHA*, 626 F.3d 84, 94 (D.C. Cir. 2010) (discussing agency's obligation under the APA to address significant comments in substantive, rather than conclusory, manner).

[53] *See* CTIA Opening Comments at 79-80.

The Proposed Rules also would have rippling effects, distorting incentives in not just directly regulated service markets, but also other product and service markets, including and especially the online advertising market. Despite repeated concerns about the role that ISPs will play in the delivery of targeted advertising, the Pro-NPRM Commenters never come to terms with the fact that ISPs currently comprise a relatively small share of the online advertising market and are the disruptive entrants with the best possibility of introducing competition to the 10 dominant, non-ISP firms that currently control 70 percent of the market.[54] Depriving ISPs of the ability to compete effectively in this market will lock them into a transmission-for-fee business model, and ultimately result in higher retail broadband prices. Moreover, as CTIA has pointed out, the only evidence of how such advertising affects consumers reveals that it is overwhelmingly positive: companies that use predictive advertising experienced a 25 percent increase in their return on investment, showing that customers prefer receiving relevant advertising and marketing communications.[55] And finally, predictive advertising often does not involve disclosure or access to a third party (*i.e.*, a loss or surrender of control) that most directly implicates customer privacy concerns. Instead, third parties seeking to deliver advertisements through ISPs can allow ISPs to create user matches in a blind manner.[56]

* * * * *

CTIA and its members appreciate and support the Commission's goal of protecting the privacy and security of broadband subscribers' data. For the reasons stated in its Opening and Reply Comments and in this letter, CTIA urges the Commission to adopt rules that distinguish between sensitive and non-sensitive data. A sensitivity-based regime is both time-tested and widely used by privacy regulators across the globe, guaranteeing strong privacy protection for consumers while preserving companies' ability to innovate. Moreover, contrary to Ohm's assertions, only such an approach will ensure that rules regarding data use and disclosure have some nexus to privacy concerns. ISPs can implement—and the Commission can enforce—this approach without difficulty. In addition, the Commission should ignore Ohm's

---

[54] *See* Swire Report at 14; CTIA Opening Comments at 94-97, 119-36; Beales Comments at 8.

[55] *See* Public Knowledge Comments at 8.

[56] *See* CTIA Opening Comments at 90-91.

exhortation to expand the scope of customer information to include both de-identified CPNI and information beyond CPNI. As explained above, this expansion is unambiguously foreclosed by the statute, its legislative history, well-established First Amendment doctrine, and strong public policy considerations. Finally, the Commission also should disregard suggestions by Ohm, OTI, and Public Knowledge to adopt rules to address theoretical or hypothetical privacy harms for which there is no evidence in the record.

Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed in ECFS. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

/s/ Scott K. Bergmann

Scott K. Bergmann
Vice President, Regulatory Affairs

Maria L. Kirby
Assistant Vice President, Regulatory Affairs &
Associate General Counsel
CTIA